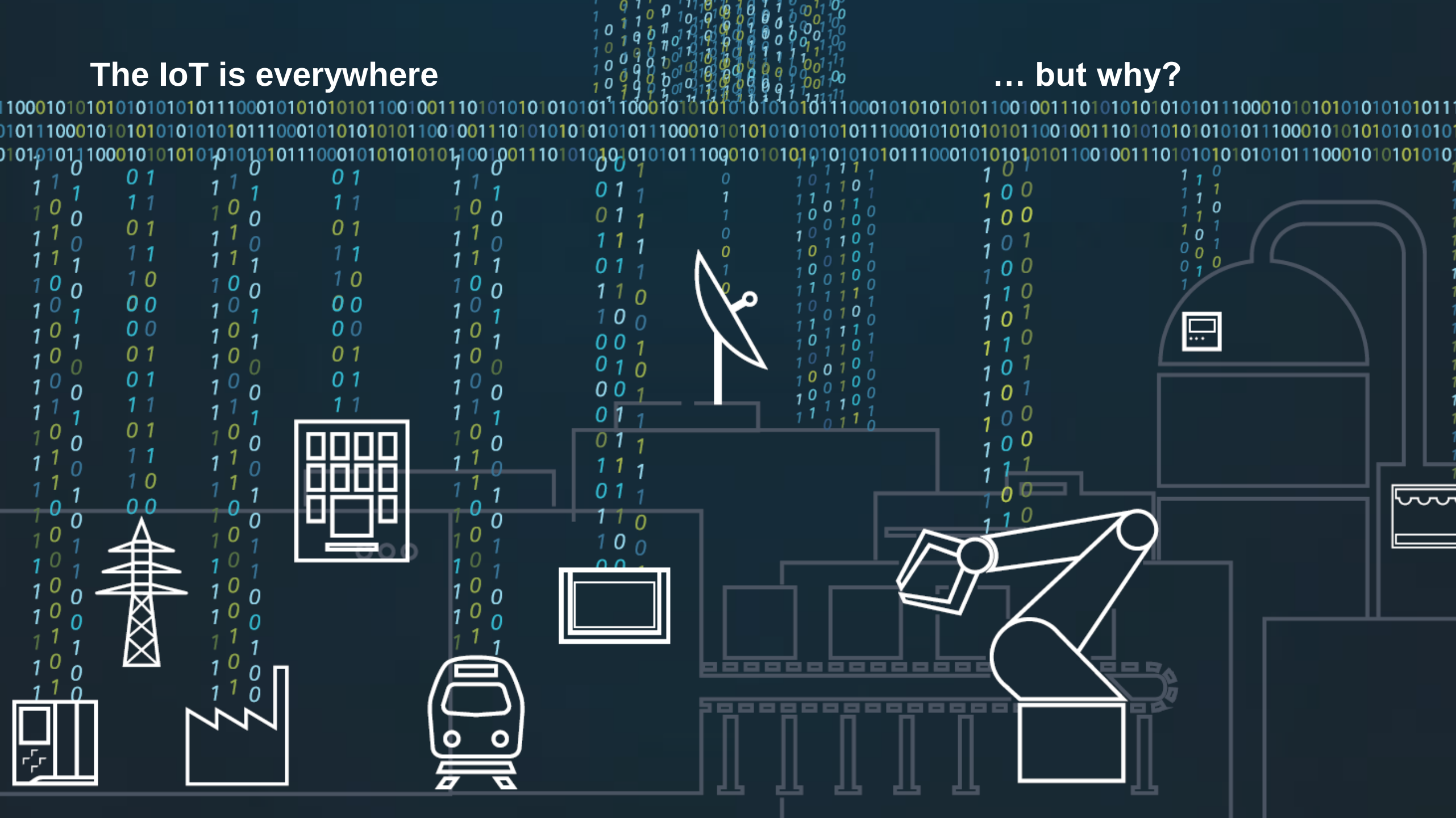
SIEMENS
Ingenuity for life

IoT Security – A joint approach

TROOPERS
MAKE THE WORLD A SAFER PLACE

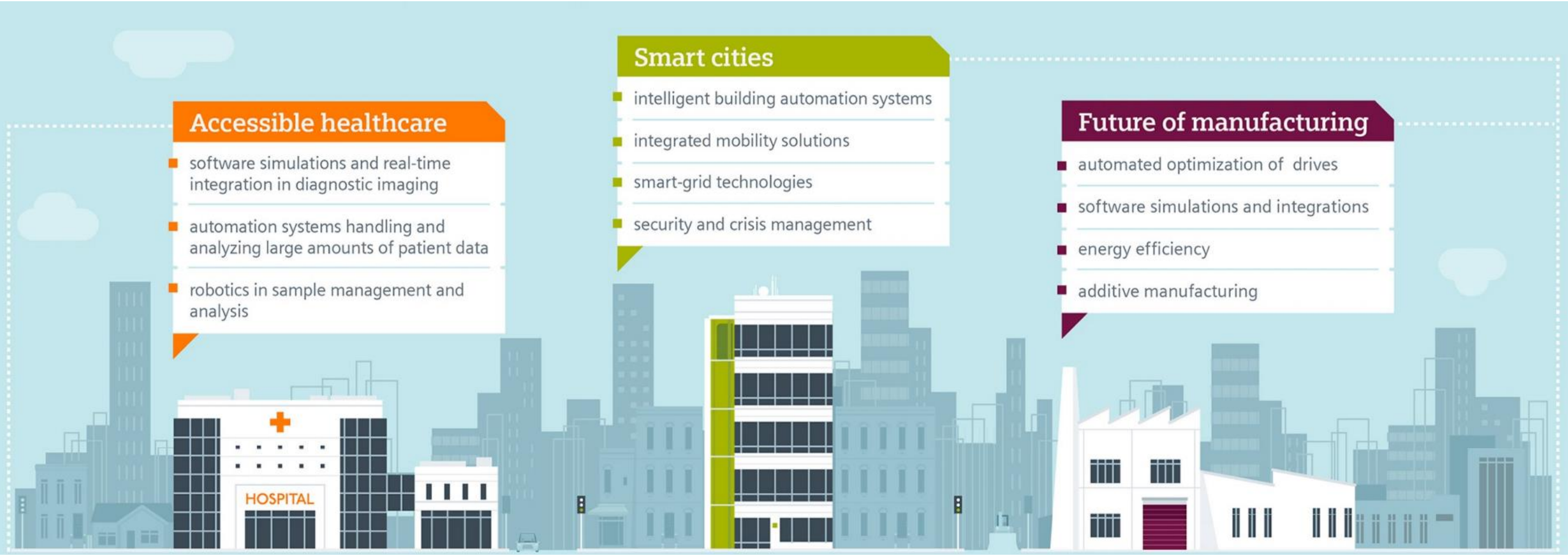
The IoT is everywhere

… but why?



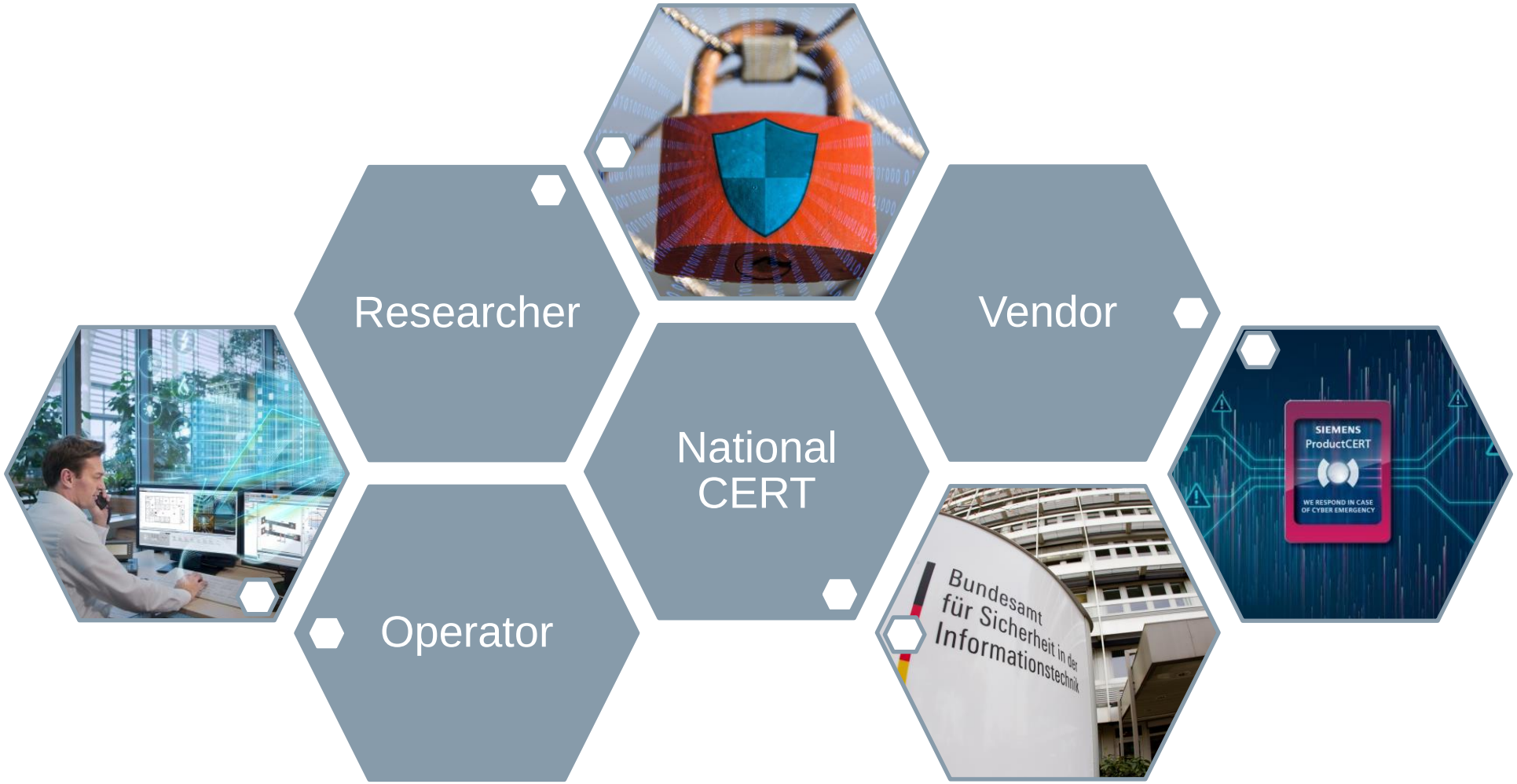
Connectivity & Digitalization help your business

SIEMENS
Ingenuity for life



Some key players in IoT security…

SIEMENS
Ingenuity for life

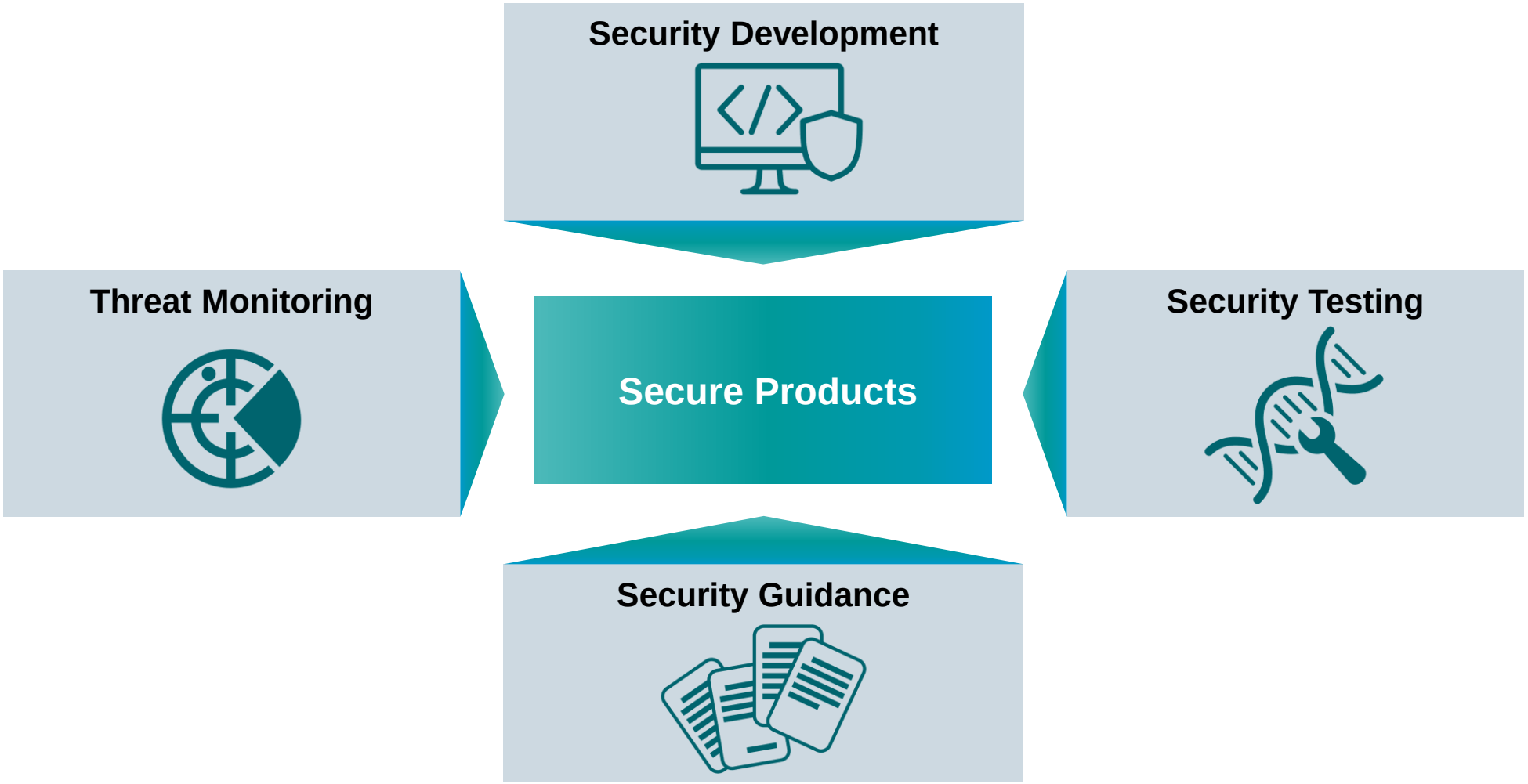


…and all of them are responsible for their own domain!

The role of the vendor

How vendors supply secure products

SIEMENS
Ingenuity for life



Roles of CSIRT & PSIRT

SIEMENS
Ingenuity for life

CSIRT

A computer security incident response team (CSIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. CSIRTs can be created for nation states or economies, governments, commercial organizations, educational institutions, and even non-profit entities. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening. (US-CERT.GOV)

PSIRT

A Product Security Incident Response Team (PSIRT) is an entity within an organization which, at its core, focuses on the identification, assessment and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components and/or services, which an organization produces and/or sells. (FIRST.ORG)

Security needs a holistic approach

SIEMENS
Ingenuity for life

CorporateCERT

- Incident Response in Large Scale Enterprise Environments
- Outstanding Forensic Capabilities
- Large CERT Community Network
- Leading in Threat Intelligence
- FIRST Membership

CustomerCERT

Bringing Experience Together, Creating Synergies and Leveraging Knowledge

Unique Combination of Skills

Leveraging 20 years CERT experience

Process Excellence

Cross Domain Knowhow

ProductCERT

- Vulnerability Handling of Siemens Products and Solutions
- Close Contact to Security Researchers
- Close Contact to Industrial CERT Community

Protect our networks — **Protect our customers' operations** — **Protect our products**

The role of the researcher

Researcher help identify issues

SIEMENS
Ingenuity for life

SIEMENS

Search for...

Hall of Thanks

Siemens expresses its sincere thanks to all individuals ethically reporting security issues in Siemens' products, solutions, or services.

Report a Security Issue

Acknowledgements

Each name represents an individual or organization who has privately reported one or more security vulnerabilities in Siemens' products, solution, services, or infrastructure and worked with Siemens to mitigate the issue.

2018

Can Demirel
Biznet Bilisim

Melih Berk Eksioglu
Biznet Bilisim

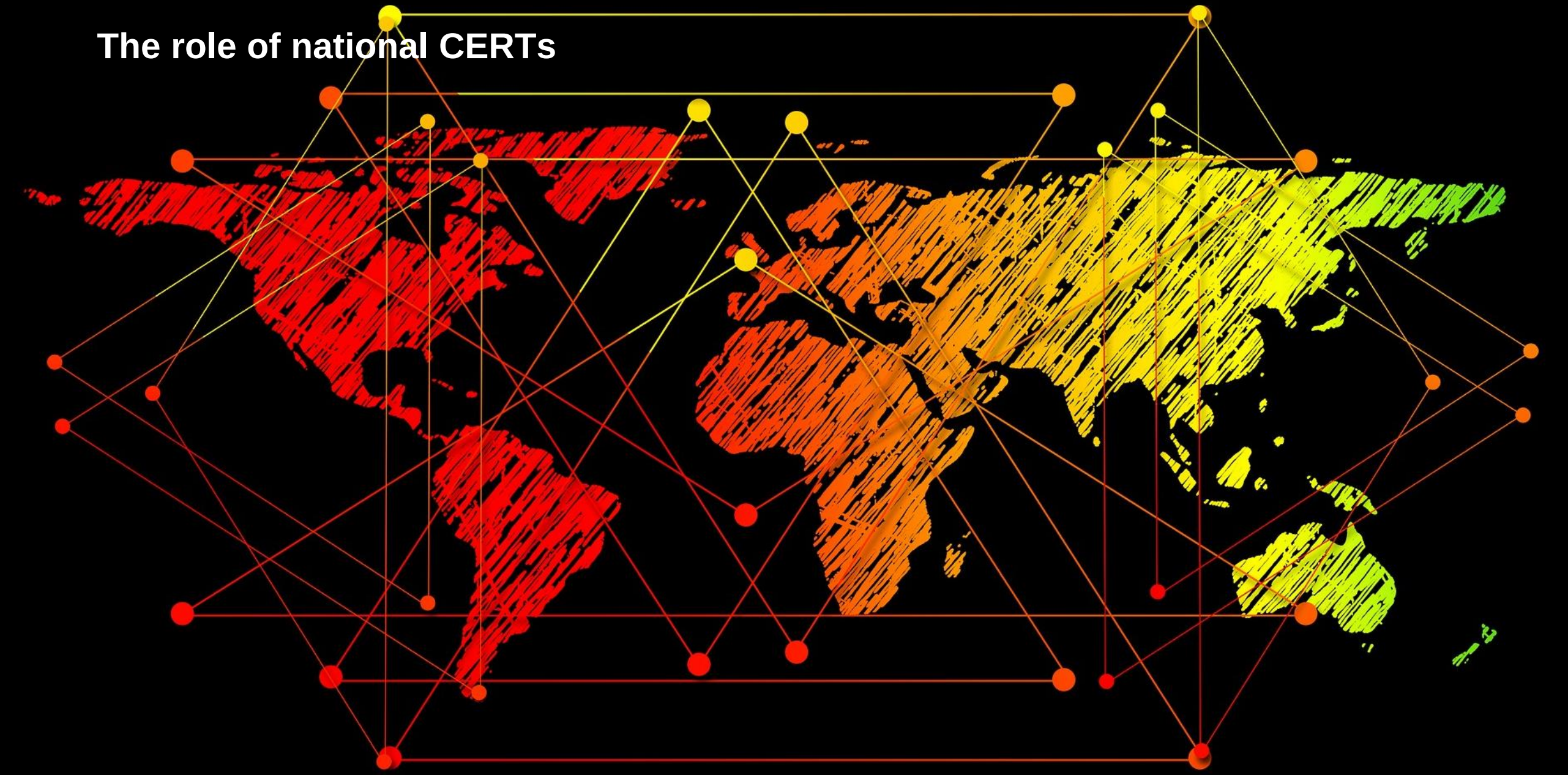
ACKNOWLEDGMENTS

(example from recent Advisory)

Siemens thanks the following parties for their efforts:

- Can Demirel and Melih Berk Ekşioğlu from Biznet Bilişim for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

The role of national CERTs



National CERTs and Coordination Teams

SIEMENS
Ingenuity for life

Vulnerabilities

- National CERTs are important contact points to researchers as they are independent from vendors.
- Vulnerability coordination teams facilitate a coordinated response amongst vendors affected by a shared issue (e.g. library).
- Advisory dissemination is an important task for national CERTs as they have the necessary channels and outreach to spread the word to operators.

Incidents

- National CERTs get informed about security related incidents within their realm and can create and share current threat information accordingly.
- National CERTs can leverage their authority to contact affected operators that would else go un-notified (e.g. through ISPs).

The role of the operator

Why is the operator so important?

SIEMENS
Ingenuity for life

Attackers Alter Water Treatment Systems in Utility Hack: Report

By Eduard Kovacs on March 22, 2016

They immediately noticed that the organization had a poor security architecture, with Internet-facing systems plagued by high-risk vulnerabilities known to be exploited in the wild, and outdated operation technology (OT) systems that had been more than ten years old.

NEWS February 8, 2018 @ 7:19 AM

Industrial Control Systems Storm the Internet, Increase Corporate Risk

By Douglas Bonderud

U.S. Has Most Internet Connected Industrial Control Systems

By SecurityWeek News on July 11, 2016

AW DAM —

Vulnerable industrial controls directly connected to Internet? Why not?

Even some devices with patches available are connected to the naked Internet.

SEAN GALLAGHER - 1/26/2018, 1:11 AM

Defense-in-Depth strengthens the operator's posture

SIEMENS
Ingenuity for life

"**Defense in Depth** employs a holistic approach to protect all assets, while taking into consideration its interconnections and dependencies, and using an organization's available resources to **provide effective layers** of monitoring and protection based on the business's exposure to cybersecurity risks."[1]

[1]NCCIC, ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 2016

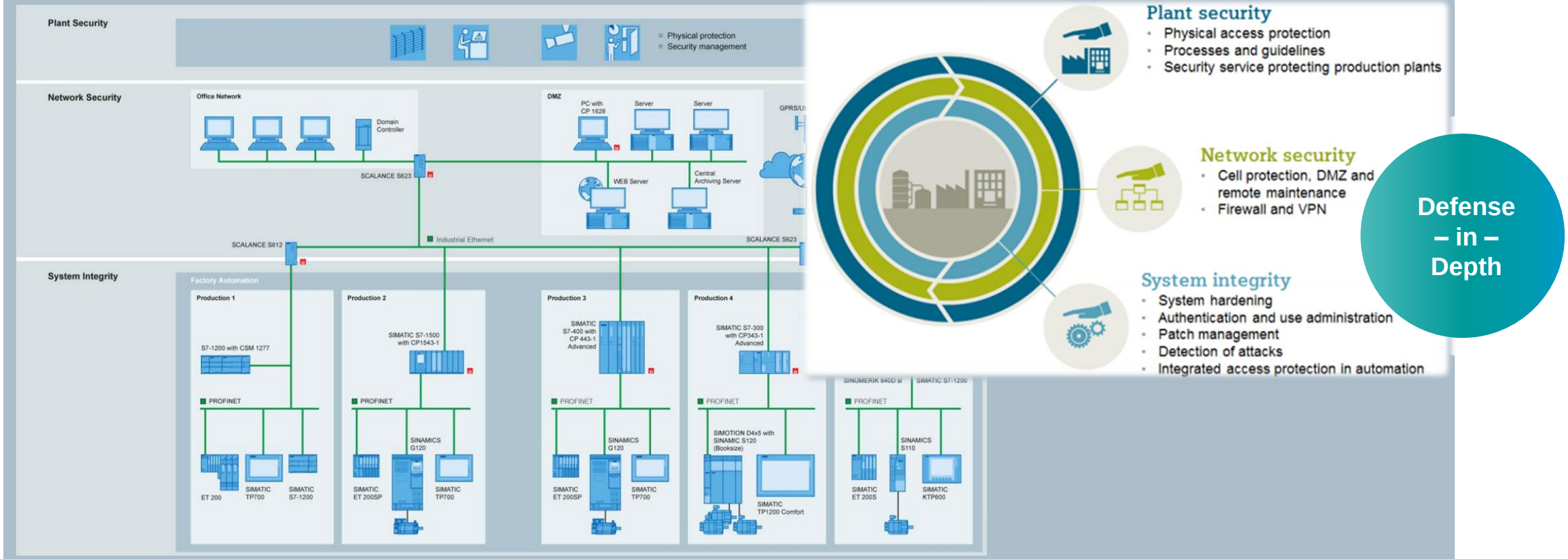
Support by Vendors Available

Defense in Depth Strategy Elements	
Risk Management Program	· Identify Threats · Characterize Risk · Maintain Asset Inventory
Cybersecurity Architecture	· Standards/ Recommendations · Policy · Procedures
Physical Security	· Field Electronics Locked Down · Control Center Access Controls · Remote Site Video, Access Controls, Barriers
ICS Network Architecture	**· Common Architectural Zones · Demilitarized Zones (DMZ) · Virtual LANs**
ICS Network Perimeter Security	**· Firewalls/ One-Way Diodes · Remote Access & Authentication · Jump Servers/ Hosts**
Host Security	**· Patch and Vulnerability Management · Field Devices · Virtual Machines**
Security Monitoring	**· Intrusion Detection Systems · Security Audit Logging · Security Incident and Event Monitoring**
Vendor Management	**· Supply Chain Management · Managed Services/ Outsourcing · Leveraging Cloud Services**
The Human Element	· Policies · Procedures · Training and Awareness

Example of Defense-in-Depth resources:

SIEMENS
Ingenuity for life

Digital Factory (Network Perspective)



Defense – in – Depth

Example of Defense-in-Depth resources:

SIEMENS
Ingenuity for life

Digital Factory (Device Perspective)

Defense – in – Depth

Example of Defense-in-Depth resources:

SIEMENS
Ingenuity for life

Energy Management

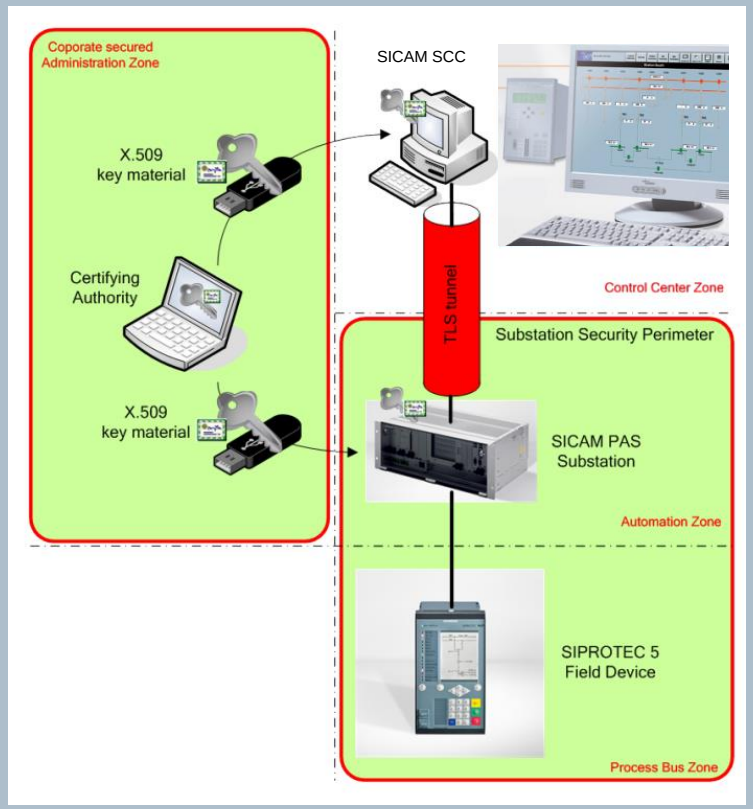
SIEMENS

SICAM/SIPROTEC

System Hardening for Substation Automation and Protection

V1.11

Guideline (Best-Practice Guide)



Defense – in – Depth

Example of Defense-in-Depth resources:

SIEMENS
Ingenuity for life

Building Technologies

Contents

Defense – in – Depth

Cybersecurity –
A critical factor for the success of the digital economy

SIEMENS
Ingenuity for life

KEY PRINCIPLES

Charter of Trust for a secure digital world

charter-of-trust.com

1. Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "It is everyone's task".

2. Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as

- **Identity and access management:** Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
- **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate.
- **Continuous protection:** Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

3. Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

4. User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer's cybersecurity needs, impacts, and risks.

5. Innovation and co-creation

Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.a. contractual Public Private Partnerships.

6. Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and trainings – in order to lead the transformation of skills and job profiles needed for the future.

7. Certification for critical infrastructure and solutions

Companies and – if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions.

8. Transparency and response

Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice which is focusing on critical infrastructure.

9. Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs).

10. Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay.

SIEMENS
Ingenuity for life

Thank You!
For keeping our communities safe and secure!